1. A method comprising:

selecting an elliptic curve method;

executing a point modification algorithm to manipulate points of the elliptic curve method;

generating a signal having a distinct characteristic using the selected elliptic curve method;

providing substantive content; and

manipulating the substantive content using the distinct characteristic.

2. The method of claim 1, wherein the point modification algorithm is selected from point addition, point subtraction, point fractioning, point multiplying, rotating, negative point modification, and a combination of one or more thereof.

3. The method of claim 1, wherein manipulating the substantive content comprises encrypting the substantive content.

4. The method of claim 1, wherein manipulating the substantive content comprises decrypting the substantive content.

5. The method of claim 1, wherein the distinct characteristic is selected from a key and a signature.

6. The method of claim 2, wherein point fractioning is selected from integral point fractioning, corresponding to a denominator that is an integral number.

7. The method of claim 2, wherein point multiplying is selected from integral multiplication, imaginary multiplication, and complex multiplication.

8. The method of claim 1, further comprising dynamically specifying the point modification algorithm in lieu of specifying the modification operation in advance.

9. The method of claim 2, further comprising selecting a first point for execution of the point modification algorithm, based on a selected property.

10. The method of claim 9, wherein the selected property is a membership condition placing the first point in a subgroup.

11. The method of claim 10, further comprising repeating the point modification algorithm with a second point selected by another entity selected from a deterministic process, a random process, and a third party.

12. The method of claim 11, wherein the second point is communicated to the point modification algorithm in a format selected from a message and a certificate.

13. The method of claim 2, further comprising selecting a first point and pre-modifying the first point by a modification operation configured to compensate for some of the processing steps, added and corresponding to execution of a series of steps in accordance with the method.

14. The method of claim 1, further comprising sending by a sender and receiving by a receiver the substantive content, and wherein the sender executes a first operation during modification for encryption and the receiver executes a second and distinct operation during modification for decryption.

15. The method of claim 1, wherein generating the distinct characteristic further comprises creating a distinct characteristic selected from a symmetric key configured to be shared by two or more parties, a decryption code for processing an encrypted signal, a digital signature, an asymmetric key, and an authentication.

16. The method of claim 1, further comprising selecting a point and wherein the point is of a type selected from a hyperelliptic curve, an algebraic curve, and abelian variety.

17. The method of claim 1, wherein modifying a point further comprises halving a point represented in a cartesian space and a point existing in a mapped cartesian space having a cartesian representation.

18. The method of claim 17, wherein halving further comprises executing a single multiplication per halving operation.

19. The method of claim 18, further comprising selecting a point characterized by a cartesian tuple and completing halving using no more than two field multiplications.

20. The method of claim 19, wherein halving further comprises negative halving including computation of a minus one-half multiple.

21. The method of claim 1, further comprising computing a fractional multiple of a point selected from a proper fraction, an improper fraction, and a complex fractional multiple.

22. The method of claim 18, further comprising determining a selection of points to execute a halving operation with respect to, based on testing for membership in a subgroup.

23. The method of claim 22, wherein testing further comprises reliance on a bit mask of coordinates corresponding to points in the subgroup.

24. The method of claim 23, wherein testing is executed by testing whether a halving procedure can be executed an arbitrary number of times selected by a user.

25. The method of claim 24, further comprising determining which of a selected number of points is to be used.

26. An apparatus comprising:

a system for creating a distinct characteristic configured to support cryptographic manipulation of information;

a memory device operably connected to the system for storing the distinct characteristic and executables programmed to operate on the distinct characteristic;

an encrypting device operably connected to the system for controlling an encryption process using the distinct characteristic;

the system further configured to execute an elliptic curve method for generating the distinct characteristic; and

the system further configured to execute a point modification algorithm for generating the distinct characteristic.

27. The apparatus of claim 26, wherein the point modification algorithm is selected from point addition, point subtraction, point fractioning, point multiplying, rotating, negative point modification, and a combination of one or more thereof.

28. The apparatus of claim 26, wherein the distinct characteristic is configured to be processable by the system for divulging independently to two independent parties a secret to be shared by the two independent parties.

29. An article comprising a computer-readable memory storing operational and executable data, the operational and executable data comprising:

an encryption engine for operating on distinct characteristics configured to encrypt substantive content representing information;

the encryption engine, further comprising a distinct characteristic generation module for operating on the distinct characteristics;

the distinct characteristic generation module, further comprising an elliptic curve module for providing the distinct characteristics; and

the elliptic curve module, further comprising a point modification algorithm for calculating points related to the distinct characteristic.

30. The article of claim 29, wherein the point modification algorithm is selected from point addition, point subtraction, point fractioning, point multiplying, rotating, negative point modification, and a combination of one or more thereof.

31. The article of claim 30, wherein point fractioning is selected from integral point fractioning, corresponding to a denominator that is an integral number.

32. The article of claim 30, wherein point multiplying is selected from integral multiplication, imaginary multiplication, and complex multiplication.

33. The article of claim 29, further comprising dynamically specifying the point modification algorithm in lieu of specifying the modification operation in advance.

34. The article of claim 30, further comprising selecting a first point for execution of the point modification algorithm, based on a selected property.

35. The article of claim 29, wherein the distinct characteristics are selected from a key and a signature.